The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A system for detecting and managing intrusion to a computer network from an unknown wireless device, the system comprising:

a security component residing on the computer network that:

passively monitors for network traffic received from an unknown wireless device;

creates a device profile of the unknown wireless device;

determines whether the unknown wireless device is an authorized device; and

if the unknown wireless device is determined to be an authorized device, permits the network traffic from the unknown wireless device to pass to the computer network.

2. The computer network system of Claim 1, wherein the security component creates a device profile of the unknown wireless device by examining identifying characteristics of the network traffic of the unknown wireless device.

3. The system of Claim 1, wherein the security component creates a device profile of the unknown wireless device by submitting at least one query to the unknown wireless device and examining the responses received as a result of the at least one query for identifying characteristics of the unknown wireless device.

4. The system of Claim 3, wherein the security component further creates the device profile of the unknown wireless device by submitting at least one subsequent query to the unknown wireless device based on a characteristic identified in a previously received response, and examining the responses received as a result of the at least one subsequent query for identifying characteristics of the unknown wireless device.

5. The system of Claim 4, wherein the characteristic identified in the previously received response is the operating system of the unknown wireless device.

6. The system of Claim 3, wherein the identifying characteristics of the unknown wireless device is the operating system of the unknown wireless device.

7. The system of Claim 3, wherein the identifying characteristics of the unknown wireless device is the MAC address of the unknown wireless device.

8. The system of Claim 3, wherein the identifying characteristics of the unknown wireless device is the TCP/IP address range of the unknown wireless device.

9. The system of Claim 3, wherein the at least one query is a standard network query.

10. The system of Claim 9, wherein the standard network query is a TCP/IP command.

11. The system of Claim 9, wherein the standard network query is a SNMP command.

12. The system of Claim 1, wherein the network traffic is from the unknown wireless device operating in an IEEE 802.11-based wireless network.

13. The system of Claim 1 further comprising a device profile database that stores known wireless device profiles.

14. The system of Claim 13, wherein the security component determines whether the unknown wireless device is an authorized device by comparing the device profile of the unknown wireless device to device profiles in the device profile database.

15. The system of Claim 14, wherein if the device profile of the unknown wireless device is not found in the device profile database, the security component associates a threat level with the unknown wireless device according to the unknown wireless device's device profile and network activity.

16. The system of Claim 15, wherein the security component de-authorizes the unknown wireless device if the threat level associated with the unknown wireless device exceeds a predetermined threshold.

17. The system of Claim 16, wherein the security component does not permit the network traffic from the unknown wireless device to pass to the computer network if the unknown wireless device is de-authorized.

18. A computer-implemented method for detecting intrusions to a computer network, comprising:

passively monitoring for network traffic received from an unknown wireless device, and upon detecting network traffic from the unknown wireless device:

creating a device profile of the unknown wireless device;

determining whether the unknown wireless device is an authorized device; and

if the unknown wireless device is determined to be an authorized device, permitting the network traffic from the unknown wireless device to pass to the computer network.

19. The method of Claim 18, wherein creating a device profile of the unknown wireless device comprises gathering identifying characteristics from the network traffic of the unknown wireless device.

20. The method of Claim 18, wherein creating a device profile of the unknown wireless device comprises submitting at least one query to the unknown wireless device and gathering identifying characteristics from the responses received as a result of the at least one query.

21. The method of Claim 20, wherein creating a device profile of the unknown wireless device further comprises submitting at least one subsequent query to the unknown wireless device based on an identifying characteristic gathered from a previously received response, and gathering additional identifying characteristics from the responses received as a result of the at least one subsequent query.

22. The method of Claim 21, wherein the identifying characteristic from the previously received response is the operating system of the unknown wireless device.

23. The method of Claim 20, wherein the identifying characteristic from the responses received as a result of the at least one query is the operating system of the unknown wireless device.

24. The method of Claim 20, wherein the identifying characteristic from the responses received as a result of the at least one query is the MAC address of the unknown wireless device.

25. The method of Claim 20, wherein the identifying characteristic from the responses received as a result of the at least one query is the TCP/IP address range of the unknown wireless device.

26. The method of Claim 20, wherein the at least one query is a standard network query.

27. The method of Claim 26, wherein the standard network query is a TCP/IP command.

28. The method of Claim 26, wherein the standard network query is a SNMP command.

29. The method of Claim 18, wherein the network traffic is from the unknown wireless device operating in an IEEE 802.11-based wireless network.

30. The method of Claim 18, wherein determining whether the unknown wireless device is an authorized device comprises comparing the device profile of the unknown wireless device to device profiles in a device profile database.

31. The method of Claim 30, wherein if the device profile of the unknown wireless device is not found in the device profile database, establishing a threat level for the unknown wireless device according to the unknown wireless device's device profile and network activity.

32. The method of Claim 31 further comprising de-authorizing the unknown wireless device if the threat level established for the unknown wireless device exceeds a predetermined threshold.

33. The method of Claim 32 further comprising not permitting the network traffic from the unknown wireless device to pass to the computer network if the unknown wireless device is de-authorized.

34. A computer-readable medium having computer-executable instructions which, when executed, carry out the method for monitoring for detecting intrusions to a computer network, comprising:

passively monitoring for network traffic received an unknown wireless device, and upon detecting network traffic from the unknown wireless device:

creating a device profile of the unknown wireless device;

determining whether the unknown wireless device is an authorized device; and

if the unknown wireless device is determined to be an authorized device, permitting the network traffic from the unknown wireless device to pass to the computer network.

35. The method of Claim 34, wherein creating a device profile of the unknown wireless device comprises submitting at least one query to the unknown wireless device and gathering identifying characteristics from the responses received as a result of the at least one query.

36. The method of Claim 35, wherein creating a device profile of the unknown wireless device further comprises submitting at least one subsequent query to the unknown wireless device based on an identifying characteristic gathered from a previously received response, and gathering additional identifying characteristics from the responses received as a result of the at least one subsequent query.

37. The method of Claim 35, wherein the at least one query is a standard network query.

38. The method of Claim 34, wherein determining whether the unknown wireless device is an authorized device comprises comparing the device profile of the unknown wireless device to device profiles in a device profile database.

39. The method of Claim 38, wherein if the device profile of the unknown wireless device is not found in the device profile database, establishing a threat level for the unknown wireless device according to the unknown wireless device's device profile and network activity.

40. The method of Claim 39 further comprising de-authorizing the unknown wireless device if the threat level established for the unknown wireless device exceeds a predetermined threshold.

41. The method of Claim 40 further comprising not permitting the network traffic from the unknown wireless device to pass to the computer network if the unknown wireless device is de-authorized.

42. A system for detecting unauthorized wireless access points on a computer network, the system comprising:

a security component residing on the computer network that:

passively monitors for network traffic from an unknown wireless device;

creates a device profile of the unknown wireless device;

determines whether the unknown wireless device is, or may be, a wireless access point according to the device profile;

if the unknown wireless device is, or may be, a wireless access point, compares the device profile of the unknown wireless device against device profiles of authorized wireless access points to determine whether the unknown wireless device is an authorized wireless access point; and

if the unknown wireless device is not determined to be an authorized wireless access point, generates an alert that the unknown wireless device is or may be an unauthorized wireless access point.

43. The system of Claim 42, wherein the security component creates a device profile of the unknown wireless device by examining identifying characteristics of the network traffic from the unknown wireless device.

44. The system of Claim 42, wherein the security component creates the device profile of the unknown wireless device by submitting at least one query to the

unknown wireless device and examining information received in response to the at least one query for identifying characteristics of the unknown wireless device.

45. The system of Claim 44, wherein the security component further creates the device profile of the unknown wireless device by submitting at least one subsequent query to the unknown wireless device based on an identifying characteristic from previously received response, and examining the information received in response to the at least one subsequent query for identifying characteristics of the unknown wireless device.

46. The system of Claim 44, wherein the identifying characteristics of the unknown wireless device is the operating system of the unknown wireless device.

47. The system of Claim 44, wherein the identifying characteristics of the unknown wireless device is the MAC address of the unknown wireless device.

48. The system of Claim 47, wherein the security component determines whether the unknown wireless device is, or may be, a wireless access point according to the device profile by examining the MAC address of the unknown wireless device.

49. The system of Claim 44, wherein the identifying characteristics of the unknown wireless device is the TCP/IP address range of the unknown wireless device.

50. The system of Claim 47, wherein the security component determines whether the unknown wireless device is, or may be, a wireless access point according to the device profile by examining the TCP/IP address range of the unknown wireless device.

51. The system of Claim 44, wherein the at least one query is a standard network query.

52. The system of Claim 51, wherein the standard network query is a TCP/IP command.

53. The system of Claim 51, wherein the standard network query is a SNMP command.

54. A computer implemented method for detecting unauthorized wireless access points on a computer network, the method comprising:

passively monitoring for network traffic from an unknown wireless device; and

upon detecting network traffic from the unknown wireless device:

creating a device profile of the unknown wireless device;

determining whether the unknown wireless device is or may be a wireless access point according to the device profile; and

if the unknown wireless device is or may be a wireless access point:

comparing the device profile of the unknown wireless device against device profiles of authorized wireless access points to determine whether the unknown wireless device is an authorized wireless access point; and

generates an alert that the unknown wireless device is, or may be, an unauthorized wireless access point if the unknown wireless device is not determined to be an authorized wireless access point.

55. The method of Claim 54, wherein creating a device profile of the unknown wireless device comprises collecting identifying characteristics from the network traffic of the unknown wireless device.

56. The method of Claim 54, wherein creating a device profile of the unknown wireless device comprises submitting at least one query to the unknown wireless device and collecting identifying characteristics in the information received in response to the at least one query.

57. The method of Claim 56, wherein creating a device profile of the unknown wireless device further comprises submitting at least one subsequent query to the unknown wireless device based on an identifying characteristic collected from a previously received response, and collecting identifying characteristics in the information received in response to the at least one subsequent query.

58. The method of Claim 56, wherein the identifying characteristics of the unknown wireless device includes the operating system of the unknown wireless device.

59. The method of Claim 58, wherein the identifying characteristics of the unknown wireless device includes the MAC address of the unknown wireless device.

60. The method of Claim 59, wherein determining whether the unknown wireless device is or may be a wireless access point according to the device profile comprises examining the MAC address of the unknown wireless device.

61. The method of Claim 58, wherein the identifying characteristics of the unknown wireless device includes the TCP/IP address range of the unknown wireless device.

62. The method of Claim 61, wherein determining whether the unknown wireless device is or may be a wireless access point according to the device profile comprises examining the TCP/IP address of the unknown wireless device.

63. The method of Claim 56, wherein the at least one query is a standard network query.

64. The method of Claim 63, wherein the wherein the standard network query is a TCP/IP command.

65. The method of Claim 63, wherein the wherein the standard network query is a SNMP command.

66. A computer-readable medium having computer-readable instructions which, when executed, carry out a method for monitoring for and detecting unauthorized wireless access points, the method comprising:

passively monitoring for network traffic from an unknown wireless device; and

upon detecting network traffic from an unknown wireless device:

creating a device profile of the unknown wireless device;

determining whether the unknown wireless device is or may be a wireless access point according to the device profile; and

if the unknown wireless device is or may be a wireless access point:

comparing the device profile of the unknown wireless device against device profiles of authorized wireless access points to determine whether the unknown wireless device is an authorized wireless access point; and

notifying a system administrator that the unknown wireless device is or may be an unauthorized wireless access point if the unknown wireless device is not determined to be an authorized wireless access point.